BILLING CODE: 6750-01-P

FEDERAL TRADE COMMISSION

[File No. 192 3003]

Support King, LLC (SpyFone.com); Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent order – embodied in the consent agreement – that would settle these allegations.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].**

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Support King, LLC (SpyFone.com); File No. 192 3003" on your comment, and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Thomas B. Carter (214-979-9372), Federal Trade Commission, Southwest Regional Office, 199 Bryan Street, Suite 2150, Dallas, TX 75201.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].** Write "Support King, LLC (SpyFone.com); File No. 192 3003" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Due to the COVID-19 pandemic and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "Support King, LLC (SpyFone.com); File No. 192 3003" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580. If possible, submit your paper comment to the Commission by overnight service.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing the proposed settlement. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before **[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].** For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Proposed Consent Order to Aid Public Comment

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Support King, LLC, formerly d/b/a SpyFone.com ("Corporate Respondent"), and Scott Zuckerman ("Individual Respondent") (collectively, "Respondents").

The Commission has placed the proposed consent order ("Proposed Order") on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received, and will decide whether it should withdraw from the agreement or make final the agreement's Proposed Order.

Support King has sold various monitoring products and services, each of which allowed a purchaser to monitor surreptitiously another person's activities on that person's mobile device. Scott Zuckerman is the president, founder, resident agent, and chief executive of Support King. Individually or in concert with others, Mr. Zuckerman controlled or had the authority to control, or participated in the acts and practices alleged in the proposed complaint.

Respondents' monitoring products and services included SpyFone for Android

Basic, Premium, Xtreme, and Xpress. These monitoring products and services had varying capabilities and costs. Purchasers of these products had to take steps to bypass numerous restrictions implemented by the operating system or the mobile device manufacturer on the monitored mobile device during installation. To enable certain functions of the monitoring products and services, purchasers had to gain administrative privileges, exposing mobile devices to various security vulnerabilities.

All of Respondents' monitoring products and services required that the purchaser have physical access to the device user's mobile device for installation, and then the purchaser could remotely monitor the device user's activities from an online dashboard. Once installed, the monitoring products and services ran surreptitiously, meaning that the device user was unaware that he or she was being monitored. The SpyFone software would then only be found by navigating through the device's "Settings," where, according to SpyFone's website, it is labeled as "System Service" in order "to be more stealthy[.]"

Device users surreptitiously monitored by Respondents' monitoring products and services could not uninstall or remove Respondents' monitoring products and services because they did not know that they were being monitored. Device users often had no way of knowing that Respondents' monitoring products and services were being used on their phones. Respondents did not take any steps to ensure that purchasers would use Respondents' monitoring products and services for legitimate purposes.

Moreover, Respondents did not take steps to secure the personal information collected from device users being monitored despite stating, "SpyFone cares about the integrity and security of your personal information. We will take all reasonable precautions to safeguard customer information, including but not limited to contact information, personally identifiable information (PII), and payment details," and "SpyFone uses its databases to store your encrypted personal information." Respondents engaged in a number of practices that, taken together, failed to provide reasonable data

security to protect the personal information collected from device users.

As a result of these unreasonable data security practices, in August 2018, an unauthorized third party accessed Respondents' server, gaining access to the data of approximately 2,200 consumers. Respondents then disseminated a notice to purchasers following the unauthorized access, representing that Respondents had "partner[ed] with leading data security firms to assist in our investigation" and that they would "coordinate with law enforcement authorities" on the matter. In reality, Respondents did not partner with any data security firms or coordinate with law enforcement authorities.

The Commission's proposed three-count complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act. The first count alleges that Respondents unfairly sell or have sold monitoring products and services that operate surreptitiously on mobile devices without taking reasonable steps to ensure that the purchasers use the monitoring products and services only for legitimate and lawful purposes.

The second count alleges Respondents deceived consumers about Respondents' data security practices by falsely representing that it would take all reasonable precautions to safeguard customer information, including by using their database to store consumers' personal information encrypted. Respondents failed to implement appropriate security procedures to protect the personal information they collected from consumers, such as by: (1) failing to encrypt personal information stored on Respondents' server; (2) failing to ensure access to Respondents' server was properly configured so that only authorized users could access consumers' personal information; (3) failing to adequately assess and address vulnerabilities of its Application Programing Interfaces (APIs); (4) transmitting purchasers' passwords for their SpyFone accounts in plain text; and (5) failing to contractually require its service provider to adopt and implement data security standards, policies, procedures or practices.

The third count alleges Respondents deceived consumers about Respondents' data breach response, when Respondents stated they were partnering with leading data security firms to investigate the data breach and coordinating with law enforcement authorities, when in fact Respondents did not.

The Proposed Order contains provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Part I of the Proposed Order requires Respondents to disable immediately all access to any information collected through a monitored mobile device, and immediately to cease collection of any data through any monitoring software. Part II requires that within 30 days of the entry of the Proposed Order, Respondents must delete all consumer data collected.

Part III of the Proposed Order requires Respondents to provide notice on all of Support King's websites, and to provide notice through emails to purchasers and trial users, stating that the FTC alleged Support King sold illegal monitoring products and services, that Support King agreed to disable the software, and that Respondents' previous notice of June 2020 was inaccurate. Respondents must also provide notice to each user of a monitored device, through an on-screen notification, informing the user that Support King collected information from his or her phone, and that the phone may not be secure.

Part IV of the Proposed Order bans Respondents from licensing, advertising, marketing, promoting, distributing, selling, or assisting in any of the former, any monitoring product or service to consumers. Part V of the Proposed Order prohibits Respondents from making any misrepresentations about the extent to which Respondents work with privacy or security firms, or the extent to which Respondents maintain and protect the privacy, security, confidentiality, and integrity of personal information. Part VI of the Proposed Order prohibits Corporate Respondent, and any Covered Business (any business controlled, directly or indirectly, by either Corporate Respondent or Individual

Respondent) from transferring, selling, sharing, collecting, maintaining, or storing personal information unless it establishes and implements, and thereafter maintains, a comprehensive information security program that protects the security, confidentiality, and integrity of such personal information.

Part VII requires Respondents to obtain initial and biennial data security assessments for twenty years for any Covered Business that collects personal information online. Part VIII of the Proposed Order requires Respondents to disclose all material facts to the assessor and prohibits Respondents from misrepresenting any fact material to the assessments required by Part VII.

Part IX requires Respondents to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program), that Respondents have implemented the requirements of the Proposed Order, are not aware of any material noncompliance that has not been corrected or disclosed to the Commission, and includes a brief description of any covered incident involving unauthorized access to or acquisition of personal information. Part X requires Respondents to submit a report to the Commission following their discovery of any covered incident.

Parts XI through XIV of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondents to provide information or documents necessary for the Commission to monitor compliance. Part XV states that the Proposed Order will remain in effect for twenty (20) years, with certain exceptions.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.

By direction of the Commission.

April J. Tabor,

Secretary.

[FR Doc. 2021-19388 Filed: 9/7/2021 8:45 am; Publication Date: 9/8/2021]